EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://team-saul.com/	Checks	9 pruebas
Dominio	team-saul.com	Hallazgos	51 totales
Fecha	27 de mayo de 2026 a las 01:56	Problemas	17 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras la auditoría técnica, el sitio web team-saul.com ha obtenido una puntuación de 68/100, lo que representa una calificación de nota C. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales 4 resultaron exitosos, 3 generaron advertencias y 2 fallos críticos. Los resultados indican deficiencias notables en la configuración de cabeceras de seguridad y en la protección de las cookies de sesión. Por todo lo anterior, el sitio se clasifica actualmente como vulnerable ante ataques de interceptación y manipulación de interfaz.

Resumen de Riesgos

0	4	11	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	50	AVISO	DHRUFUSION: falta SameSite; pagelimit: falta Htt...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 44 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  44 dias restantes (expira: 2026-07-10T03:24:11.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-11T03:24:12.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: hcdn — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://team-saul.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js, PHP/7.4.33

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 50/100

Estado: AVISO

DHRUFUSION: falta SameSite; pagelimit: falta HttpOnly; pagelimit: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: DHRUFUSION — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: DHRUFUSION — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: DHRUFUSION — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: pagelimit — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: pagelimit — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: pagelimit — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.dhru.com/?fromaid=team-saul.com

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows

- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Strict-Transport-Security: La ausencia de la cabecera HSTS permite que la conexión pueda degradarse a protocolos no cifrados.
[HIGH] X-Frame-Options: La falta de esta cabecera hace que el sitio sea vulnerable a ataques de Clickjacking.
[HIGH] Cookie pagelimit (HttpOnly): Al carecer del atributo HttpOnly, la cookie es accesible mediante scripts de cliente, aumentando el riesgo de robo de sesión vía XSS.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite al navegador realizar sniffing de tipos MIME, lo que facilita ataques de inyección.
[MEDIUM] Cookie DHRUFUSION y pagelimit (SameSite): La ausencia de este atributo expone al usuario a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectó un recurso cargado mediante el protocolo inseguro HTTP, comprometiendo la integridad del cifrado SSL.
[MEDIUM] Archivos y rutas expuestas: El acceso público a /readme.html, /README.txt y paneles de administración (/wp-login.php, /administrator/) facilita el reconocimiento a atacantes.
[MEDIUM] Referrer-Policy y Permissions-Policy: La ausencia de estas cabeceras compromete la privacidad del usuario y el control sobre las APIs del navegador.
[LOW] Exposición de tecnología: Las cabeceras Server (hcdn) y X-Powered-By (PHP/7.4.33) revelan versiones específicas que pueden usarse para buscar vulnerabilidades conocidas.
[LOW] Ausencia de Robots.txt y Sitemap: La falta de estos archivos dificulta el control de indexación y el mapeo estructurado del sitio.